

А. Д. Зобнин

студент 4-го курса,
ФГБОУ ВО «Санкт-Петербургский государственный экономический университет»

В. И. Княев

профессор кафедры Информатики,
ФГБОУ ВО «Санкт-Петербургский государственный экономический университет»

БИОМЕТРИЧЕСКИЕ ТЕХНОЛОГИИ КАК МЕХАНИЗМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЦИФРОВОЙ ЭКОНОМИКЕ

Аннотация. В статье рассматриваются возможности применения новых методов биометрических технологий для построения систем обеспечения информационной безопасности организации на этапе перехода к цифровой экономике.

Ключевые слова: информационная безопасность, биометрические технологии, цифровая экономика, цифровая платформа.

Введение

На сегодняшний день биометрия прочно вошла в нашу жизнь. Она является неотъемлемой частью рынка IT технологий, и за счет своей надежности и удобства использования играет большую роль в сфере информационной безопасности [4].

Биометрия – это технология, которая позволяет распознавать (идентифицировать) человека по его индивидуальным физическим или поведенческим чертам [6, 7]. Эти черты делят на два типа: статические - уникальные данные, которые не меняются с течением жизни (отпечатки пальцев или рисунок папиллярных линий, ДНК, сетчатка глаза) и динамические, то есть параметры, которые по тем или иным причинам могут со временем изменяться (почерк и динамика подписи, голос и ритм речи, скорость и особенности работы на клавиатуре компьютера, походка) (Рис. 1).



Рисунок 1. Биометрические параметры человека в системах идентификации и доступа

Методов идентификации, по которым можно определить человека придумали большое количество. Одними из самых распространенных являются пароль, персональные идентификационные номера (PIN) и использование документов. Однако эти способы имеют недостатки, например, пароль можно забыть, перехватить, подсмотреть, взломать. Такие системы защиты можно обойти, скомпрометировать, и в целом, они завязаны на проверке некоторого пароля, который должен знать человек, но не на распознавании самого человека [8]. Биометрические системы безопасности, которые работают в автоматическом

режиме и позволяют с большой точностью идентифицировать конкретного человека по его физиологическим или поведенческим характеристикам, помогут устранить эти и подобные проблемы: мошенникам будет недостаточно кражи пароля, документов или подделки карт, можно будет персонально предоставлять права доступа к важной информации, не будет возникать проблем, связанных с забыванием кодов или потерей карт, человек не сможет скомпрометировать пароли из-за своей невнимательности или неосторожности.

Принцип работы всех биометрических систем одинаков. Сперва один или несколько биометрических эталонных образцов записываются и преобразовываются в компьютерный код, который затем заносится в память системы. Когда требуется произвести идентификацию человека система выделяет необходимые для анализа уникальные признаки нового биометрического образца. После этого идет сравнение нового и эталонного образца и на основе этого анализа выносится решение о совпадении или несовпадении биометрических параметров. Это решение отправляется запрашиваемой системе, которая дальше сама решает, что ей предпринять.

Надежность – это главная черта биометрических систем, это значит, что система может достоверно различать биометрические параметры разных людей. Тем не менее, различные системы имеют разные коэффициенты надежности – вероятность возникновения ошибок 1-го и 2-го рода.

Ошибкой 1-го рода (FRR – False Rejection Rate) называется вероятность отказать в доступе человеку, который имеет на это право. Это может произойти при повышении порога чувствительности или по причине искажения идентификатора, например, при простуде может измениться голос человека. Такие ошибки могут происходить достаточно часто. Ошибкой 2-го рода (FAR – False Acceptance Rate) называется вероятность предоставить доступ человеку, не имеющему на это право, то есть при неверном сопоставлении образцов, когда система опознает одного человека как другого, что, безусловно, может являться критичным на некоторых защищаемых объектах.

На самом деле подделать биометрические параметры человека довольно легко по отдельности (копии отпечатков пальцев рук, формы уха, сетчатки глаза и т. д.) – но крайне трудно, если использовать сразу несколько типов биометрических характеристик. Это существенно повысит безопасность системы, так что появление ошибок 2-го рода маловероятно. Системы могут сильно различаться по вероятностям возникновения ошибок, так что придется определить, что приоритетнее – не допустить прохода возможного субъекта нелегального доступа или допустить всех своих. Не стоит забывать, что простота, скорость идентификации и стоимость системы крайне важны, ведь если человек будет испытывать неудобство каждый раз при сканировании, то ему не захочется пользоваться данной системой, поэтому придется найти баланс между данными характеристиками.

Рынок биометрии растет быстрыми темпами. Больше всего биометрические технологии востребованы в госсекторе (электронные паспорта, водительские удостоверения личности и иные документы, национальные биометрические системы), вторым по величине использования биометрии является туристический сектор (путешествия и миграция). Следом идет финансовый сектор. Безусловно, технологии биометрии понадобятся в военных учреждениях и на закрытых стратегических объектах, где принципиально важно не допустить проникновения посторонних людей. Эксперты полагают, что объем мирового рынка биометрических технологий к 2023 году составит 33\$ млрд., а среднегодовой темп роста рынка ближайшие пару лет будет равен 18%. В России этот темп в 1,6 раз превышает мировые показатели. Прогнозируется, что количество устройств, способных проводить биометрическую идентификацию человека, к 2022 году достигнет отметки в 5,5 млрд. единиц.

На данный момент более половины мирового рынка биометрических технологий приходится на отпечатки пальцев рук, а половина оставшихся использует изображение лица и рисунки вен ладоней. При этом, в ближайшие годы способ идентификации человека

по радужной оболочке глаза и голосу будут резко увеличивать свое распространение, а способ распознавания по отпечаткам пальцев замедлит свой рост.

Гипотеза

Ключевую роль в развитии, введении и применении биометрических технологий в финансовом секторе сыграл рынок мобильных телефонов. На сегодняшний день большинство смартфонов имеют сканер отпечатка пальца, что подтверждает доминирующее положение данной технологии на рынке, кроме того, с помощью телефонов можно записывать голос и делать фотографии, а некоторые и вовсе обладают встроенными сканерами сетчатки глаз [10]. Со временем будут появляться новые технологии, использующие разные типы биометрических данных и будет больше возможностей для идентификации пользователей. Будет возможно проводить проверку не одним типом биометрических параметров, а комбинацией нескольких, что существенно повысит точность идентификации и позволяет определить настоящего человека, а не его цифровую подделку.

Кроме того, технологии биометрии начинают появляться в банкоматах и терминалах самообслуживания, в магазинах получают распространение системы, которые позволяют покупателям расплатиться, просто посмотрев в камеру, а при звонках в службу поддержки пользователей применяются системы, определяющие человека по голосу, то есть такие технологии становятся повсеместными.

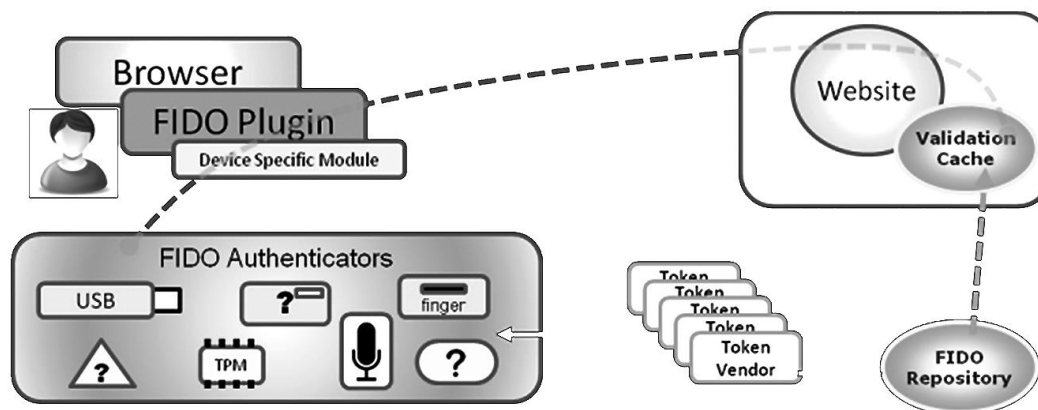


Рисунок 2. Схема использования отпечатков пальцев в продуктах альянса FIDO

С развитием мобильных технологий повысилось количество мобильных платежей. Появление на рынке надежных платёжных систем для оплаты покупок с помощью смартфона стало толчком к развитию биометрических технологий. Samsung Pay, Google Pay, Apple Pay позволяют очень просто и быстро совершать покупки в магазинах и на сайтах, что пришлось по душе многим пользователям.

Для создания открытого стандарта и распространения этой системы был образован альянс FIDO (Fast Identity Online), куда вошли компании Lenovo, PayPal, Nok Nok Labs, Validity, Agnitio, Infineon и др. (рис. 2). Стандарт FIDO вберёт в себя широкое разнообразие методов аутентификации: биометрическое, голосовое и фотографическое опознавание, существующие стандарты (например, NFC), технологии токенов и USB-ключей.

Методы

В настоящее время в России нет законов, касающихся использования биометрических технологий, выходящих за рамки применения Единой биометрической системы (ЕБС) [7, 9]. Поясним, что ЕБС — это цифровая платформа, созданная для выполнения национальной программы «Цифровая экономика Российской Федерации» и призванная упростить взаимодействие клиентов с банками [12]. Эта система позволяет производить удаленную

ИНФОРМАТИКА И ИНФОРМАЦИОННЫЕ СИСТЕМЫ

идентификацию клиентов для оказания банковских услуг, например, для перевода денежных средств, открытия счетов и вкладов или при выдаче кредитов, а в будущем с помощью системы граждане смогут получить защищенный доступ к государственным, муниципальным и коммерческими цифровым услугам и сервисам в любое время дня и ночи, из любого места мира. Применение удаленной идентификации регламентировано Федеральным законом №482-ФЗ от 31 декабря 2017 г., который вносит изменения в закон от 07.08.2001 №115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» и от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» .

Банки являются для клиентов символом надежности и доверия. Чем выше доверие к банку, тем больше средств он сможет привлечь, а это является смыслом существования кредитных организаций. Безопасность является важным свойством банковской деятельности, потребители банковских услуг должны быть убеждены в сохранности своих сбережений, в безопасности персональных данных, а уверенность в этом зависит от степени доверия к банку, его репутации, поэтому все больше внимания уделяется идентификации пользователей и сотрудников с помощью методов, использующих биометрические данные человека. Такую информация не получится потерять или забыть, и, самое главное, для проверки необходимо личное присутствие именно проверяемого клиента.

Многие банки уже давно используют биометрию в своей деятельности, к примеру, для контроля доступа и мониторинга сотрудников внутри помещений, а также для доступа к сейфам, хранилищам и депозитарным ячейкам [8]. Биометрия позволяет повысить не только безопасность персональных данных, но и секретной документации организации, кроме того, биометрические технологии могут применяться в антифрод системах, что существенно снизит уровень мошенничества и финансовых махинаций, а соответственно и уменьшит финансовые потери [5]. Антифрод-системы позволяют отслеживать аномальное поведение пользователей и блокировать подозрительные транзакции [8]. С внедрением ЕБС существенно снизится вероятность проведения мошеннических операций, причем во всех банках сразу. Благодаря объединению всех данных в одной системе мошенник не сможет воспользоваться банковскими услугами, где применяется биометрическая идентификация по личности, в какое бы отделение он не пришел. То же касается и осужденных или людей, находящихся под следствием, биометрические параметры которых будут известны и можно будет приостановить их деятельность в системе.

До появления Единой биометрической системы, для дистанционного доступа к банковским услугам, клиенту обязательно надо было лично несколько раз посетить офис интересующего его банка для прохождения процедуры идентификации [4]. Теперь же клиент имеет возможность дистанционно пользоваться услугами не одного банка, где он проходил эту процедуру, а любого, подключенного к системе. Правда, чтобы можно было воспользоваться услугами удаленной идентификации, один раз все же придется посетить отделение уполномоченного на это банка, при этом его клиентом быть не обязательно [6]. Если гражданин не был зарегистрирован на портале Госуслуг (в ЕСИА), сотрудник банка поможет это сделать, далее будет сделана фотосъемка пользователя и записан голос, после чего эти данные будут загружены в ЕБС. Хранятся биометрические образцы в системе в обезличенной форме. Регистрация граждан в ЕБС и ЕСИА является для них бесплатной и добровольной. Стоит отметить, что эти данные хранятся в системе в течение 3 лет и по истечение этого времени их будет необходимо обновить.

Работа с Единой биометрической системой началась в довольно короткие сроки. После принятия поправок в федеральные законы, уже в первой половине 2018 года банки активно начали готовить свою инфраструктуру к внедрению системы, изучать и тестировать ее, а также предлагать различные варианты по усовершенствованию механизма удаленной идентификации пользователей [6, 10]. Свыше двадцати крупных банков поучаствовали в тестировании единой биометрической системы. В середине лета 2018 года произошел

официальный запуск ЕБС и в банках началось полноценное использование данного механизма. По распоряжению правительства от 2 марта 2018 года «Ростелеком» назначен оператором ЕБС. На него возлагается ответственность за сбор, обработку и хранение биометрии, кроме того Ростелеком будет сверять полученные образцы с эталонным шаблоном. Ответ системы о соответствии биометрии будет отправлен обратно в запрашивающий проверку банк. Стоит отметить, что Ростелеком занимался созданием и поддержкой Единого портала госуслуг и ЕСИА, а также занимался разработкой ЕБС и законодательных основ, необходимых для ее создания и применения. На март 2020 года в Единой биометрической системе зарегистрировалось более 120 тысяч россиян.

Результаты и обсуждение

Единая биометрическая система была создана для развития цифровой экономики страны. После появления ЕБС увеличится количество доступных цифровых государственных и муниципальных услуг, что означает повышение общей цифровизации системы госуправления. Люди смогут получать банковские услуги независимо от времени и местоположения. Это повысит финансовую доступность для граждан из любых регионов, а также для пожилого и маломобильного населения. Также ЕБС повышает уровень конкуренции на рынке, так как клиенты получают возможность пользоваться услугами любого банка дистанционно и заключать договор с наиболее конкурентоспособной кредитной организацией. Фактически пользователи получают возможность выбирать даже не определенную организацию, а понравившийся им продукт, который она предлагает. Получается, что географическое местоположение перестает быть определяющим фактором: клиентом банка можно будет стать практически любому человеку из любого региона России. На сегодняшний день с помощью биометрии у людей есть возможность получать необходимые финансовые услуги посредством лишь смартфона, что дает так называемую цифровую свободу.

Коммерческим банкам ЕБС позволит увеличить приток клиентов, поскольку с возможностью удаленной идентификации банк сможет обслуживать клиента по Интернету независимо от их взаимного расположения [1]. А это в свою очередь поможет банку увеличить свое присутствие на рынке. Вдобавок появляется целый спектр новых цифровых услуг, соответствующих уровню развития современных технологий: оформление договоров, открытие вкладов и счетов, выдача кредитов – полноценное обслуживание клиента круглосуточно и без выходных.

Другие преимущества ЕБС для банков – это сокращение операционных издержек на обслуживание отделений, возможность автоматизировать контактные центры, снизить расходы на обслуживание клиентов. Как следствие, банки приобретают возможность потратить ресурсы на повышение качества услуг, а не на расширение сети продаж. Само собой, внедрение биометрических технологий потребует создания новой инфраструктуры, что обернется немалыми затратами для банка [3, 5]. Однако, банки, доработавшие свои системы и использующие биометрию, бесспорно, выйдут в лидеры в новой цифровой экономике. Поэтому, чтобы не проиграть конкуренцию, банки стремительно развивают цифровой бизнес. Заметим, что последние несколько лет клиенты уходят в онлайн и наблюдается снижение количества посещений банков.

При этом привлекать новых потребителей старыми способами становится все дороже и дороже. Следовательно, коммерческие банки рискуют недосчитаться большого процента прибыли уже через несколько лет, если не последуют за компаниями, активно использующими цифровые платформы и предлагающими цифровые услуги.

Внедрение системы удаленной идентификации с использованием биометрии стоит больших денег, что препятствует росту цифровой экономики, особенно это касается небольших банков в связи с недостатком ресурсов [2]. Широкое распространение таких систем в банках осложняется из-за ряда других причин. Например, существует погрешность измерения биометрических образцов в силу того, что уникальные свойства человека

меняются с течением времени из-за разных факторов. Кроме того, биологические данные могут значительно измениться и в краткий срок, к примеру, по причине болезни голос может претерпеть изменения, а волнение или стресс могут повлиять на почерк человека и его стиль набора текста на клавиатуре.

Возможность удаленной идентификации в банках – лишь первый этап цифровизации финансового сектора РФ [12]. Эта технология распространится в будущем и на другие сферы финансового рынка, к примеру, на страхование [11]. В будущем ЕБС превратится в национальную платформу для удобного и безопасного доступа ко всевозможным цифровым услугам. В дальнейшем людям станут доступны услуги в совершенно разных отраслях, как в финансовых, так и в нефинансовых. Перспективно применение системы в государственном секторе: сейчас многие услуги невозможно получить удаленно из-за того, что необходимо лично прийти получить документ, предъявив удостоверение личности. Появятся возможности в сфере образования [4], здравоохранения, ритейла, электронной коммерции, при использовании аэропортов, портов и железнодорожных вокзалов.

В заключение стоит сказать, что внедрение Единой биометрической системы требуется для полноценного перехода к цифровой экономике, которая неразрывно связана с информационной безопасностью, и принципиально иному уровню финансовой доступности. При эффективном регулировании и дальнейшем развитии системы мы выйдем на совершенно новый уровень развития. Внедрение в различные сферы экономики биометрических технологий позволит минимизировать мошенничество, существенно повысить уровень обслуживания клиентов и увеличит качество их взаимодействия с государством и бизнесом.

Список литературы

1. Барабанова М.И., Кияев В.И., Сайтов А.В. Открытые системы и сети. Комплексная безопасность в системах и сетях современного предприятия. — Учебник / под ред. проф. В. И. Кияева — СПб: Изд-во СПбГЭУ, 2019. — 412 с.
2. Винокуров А. В. Биометрические системы идентификации в кредитных организациях как инструмент противодействия мошенничеству // Финансы и кредит. — 2016. — № 21. — С.15–21.
3. Газуль С. М., Кияев В. И. Особенности построения сервиса журналирования системных событий на основе blockchain-подобной платформы и технологий виртуализации // Труды 5-й Международной научной конференции «Технологическая перспектива в рамках евразийского пространства: новые рынки и точки экономического роста». 7-8 ноября 2019 г., Санкт-Петербург, — СПб., изд-во «Астерион», 2019. — С. 237-241.
4. Газуль С.М., Ананченко И.В., Кияев В.И. Проектирование прототипа клиентского устройства для гибридной информационной системы поддержки образовательного процесса в вузе // Современные проблемы науки и образования. — 2015, — № 1; URL: www.science-education.ru/125-20219 (дата обращения: 28.05.2020).
5. Газуль С.М., Кияев В.И. Гибридные информационные системы — новые угрозы информационной безопасности // В сб. Комплексная безопасность бизнеса в условиях экономической нестабильности, 2014. — С. 97-100.
6. Достов В. Л., Шуст П. М., Козырева А. Д. Новые концепции применения риск-ориентированного подхода при осуществлении процедур идентификации // Юридическая наука. — 2017. — № 5. — С.104–112.
7. Единая биометрическая система: доступные материалы. [Электронный ресурс] URL: <https://bio.rt.ru/documents/> (дата обращения 12.04.2020).
8. Крылова И. Ю., Рудакова О. С. Биометрические технологии как механизм обеспечения информационной безопасности в цифровой экономике // Молодой ученый. — 2018. — №45. — С. 74-79. — URL <https://moluch.ru/archive/231/53640/>.
9. О единой биометрической системе. [Электронный ресурс] URL: <https://bio.rt.ru/about/> (дата обращения 17.04.2020).
10. Обзор международного рынка биометрических технологий и их применение в финансовом секторе. [Электронный ресурс] URL: http://www.cbr.ru/content/document/file/36012/rev_bio.pdf (дата обращения 15.04.2020).
11. Стратегия повышения финансовой доступности в Российской Федерации на период 2018–2020 годов. [Электронный ресурс]. URL: https://cbr.ru/content/document/file/44104/str_30032018.pdf (дата обращения 15.04.2020).
12. Цифровая конвергенция в экономике / [В.В. Трофимов и др.]; под ред. В.В. Трофимова, В.Ф. Минакова. — СПб. : Изд-во СПбГЭУ, 2019. — 150 с.